IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

MICHELLE CLARK, individually and on behalf of all others similarly situated, Plaintiff, v. **CITRIX SYSTEMS, INC.**, Defendant.	Case No.: CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Michelle Clark, individually and on behalf of all similarly situated persons, alleges the following against Citrix Systems, Inc. ("Citrix") based on personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents, as to all other matters:

INTRODUCTION

1. Plaintiff brings this class action against Citrix for its failure to properly secure and safeguard Plaintiff's and other similarly situated customers' ("Class Members," as defined *infra*) sensitive information, including, in the case of customers of Comcast Cable Communications, LLC d/b/a Xfinity ("Xfinity"), names, contact information, last four digits of Social Security numbers, dates of birth and/or secret questions and answers ("personally identifiable information" or "PII").

2. Citrix provides cloud computing services to over 16 million cloud users, and makes a variety of software products, including networking products.[1]

[1] https://www.citrix.com/about/

3. Plaintiff is a customer of Xfinity for a home internet package, which used software provided by Citrix in October of 2023.[2]

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Citrix assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On October 10, 2023, Citrix published a security bulletin entitled "NetScalerADC and NetScaler Gateway Security Bulletin for CVE-2023-4966 and CVE-2023-4967" which announced "Multiple vulnerabilities have been discovered in NetScaler ADC (formerly Citrix ADC) and NetScaler Gateway (formerly Citrix Gateway)."[3] This vulnerability has become known as "Citrix Bleed".[4]

6. According to a leading cybersecurity and threat intelligence company, Mandiant, it has identified exploitation of the vulnerability "in the wild" beginning in August of 2023 and it is investigating "multiple instances of successful exploitation of CVE-2023-4966 that resulted in the takeover of legitimate user sessions on NetScaler ADC and Gateway appliances. The session takeovers bypassed password and multi-factor authentication."[5]

7. According to Mandiant, it is currently "investigating intrusions across multiple verticals, including legal and professional services, technology, and government organizations. Given the widespread adoption of Citrix in enterprises globally, we suspect the number of impacted

---

[2] *See* Notice of Breach emailed to Plaintiff, attached as Exhibit A.
[3] https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967 (last accessed January 5, 2024)
[4] https://www.cisa.gov/guidance-addressing-citrix-netscaler-adc-and-gateway-vulnerability-cve-2023-4966-citrix-bleed (last accessed January 5, 2024)
[5] https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966 (last accessed January 5, 2024)

organizations is far greater and in several sectors. The victims have been in the Americas, EMEA, and APJ as of writing."[6]

8. Xfinity, in response to additional mitigation guidance provided by Citrix on October 23, 2023, claims it "promptly patched and mitigated [its] systems," however, despite that action, Xfinity "subsequently discovered that prior to mitigation, between October 16 and October 19, 2023, there was unauthorized access to some of [Xfinity's] internal systems that [Xfinity] concluded was a result of this vulnerability." [7] In a filing with the Office of the Maine Attorney General, Xfinity revealed that the PII of 35,879,455 individuals is believed to have been exposed by the Data Breach.[8]

9. Citrix failed to adequately protect Plaintiff's and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Citrix's negligent and/or careless acts and omissions and its utter failure to protect its clients' customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Citrix's failure to:

(i) adequately protect the PII of Plaintiff and Class Members;

---

[6] *Id.*
[7] *See* Data Breach Notice, Exhibit A.
[8] https://apps.web.maine.gov/online/aeviewer/ME/40/49e711c6-e27c-4340-867c-9a529ab3ca2c.shtml (last accessed January 5, 2024)

(ii) warn Plaintiff and Class Members of Citrix's inadequate information security practices; and

(iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents.

Citrix's conduct amounts at least to negligence and violates federal and state statutes.

11. Citrix disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures and ensure those measures were followed by its IT vendors to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

12. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

13. Plaintiff and Class Members have suffered injury as a result of Citrix's conduct. These injuries include:

(i) invasion of privacy;

(ii) lost or diminished value of PII;

(iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach;

(iv) loss of benefit of the bargain;

(v) an increase in spam calls, texts, and/or emails; and

(vi) the continued and certainly increased risk to their PII, which:

(a) remains unencrypted and available for unauthorized third parties to access and abuse; and

(b) remains backed up in Citrix's possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the PII.

14. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Citrix's inadequate data security practices.

PARTIES

15. Plaintiff Michelle Clark is, and at all times mentioned herein was, an individual citizen and resident of Camden County, New Jersey.

16. Defendant Citrix is a corporation validly existing and organized under the laws of Delaware with its headquarters and principal place of business located at 851 W. Cypress Creek Road, Fort Lauderdale, Florida 33309.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is in the millions, many of whom reside outside the state of Florida and have different citizenship from Citrix, including Plaintiff. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

18. This Court has general personal jurisdiction over Citrix because it is headquartered in this District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to this action occurred in this District, Citrix has harmed Class Members residing in this District, and Citrix is subject to the Court's personal jurisdiction with respect to this action.

FACTUAL ALLEGATIONS

20. Citrix is a multinational private corporation that sells cloud and networking software. Xfinity sells cable television and Internet services.

21. Plaintiff and Class Members are current and former customers of companies that use Citrix products, including Xfinity, who provided their PII to those companies as a condition of obtaining services.

22. The information held by Citrix in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

23. Upon information and belief, Xfinity made promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them would be kept safe, confidential, that the privacy of that information would be maintained, and that their sensitive information would be deleted after it was no longer needed.

24. Plaintiff and Class Members provided their PII to Xfinity with the reasonable expectation and on the mutual understanding that Xfinity and its software providers, including Citrix, would comply with their obligations to keep such information confidential and secure from unauthorized access.

25. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Citrix to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

26. Citrix had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of their IT vendors and affiliates. Citrix has a legal duty to keep consumer's PII safe and confidential.

27. Citrix had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

28. Citrix derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Citrix could not perform the services they provide.

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Citrix assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

30. According to the Notice, Citrix announced the vulnerability on October 10, 2023, but did not issue additional mitigation guidance until October 23, 2023.[9]

31. Omitted from the Notice are the details of the root cause of the Data Breach, the vulnerabilities exploited, and the specific remedial measures undertaken to ensure such a breach

[9] Data Breach Notice, Exhibit A.

does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

32. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

33. Citrix did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed. Moreover, Citrix failed to exercise due diligence in selecting its vendors or deciding with whom they would share sensitive PII.

34. The attacker accessed and acquired files containing unencrypted PII of Plaintiff and Class Members, including their names, dates of birth, and Social Security numbers. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

35. Plaintiff further believes her PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type. Moreover, following the Data Breach, Plaintiff has experienced suspicious spam and believes this be an attempt to secure additional PII from her.

36. Citrix derives a substantial economic benefit from providing software for its clients, including Xfinity, and as a part of providing that software, Citrix retains and stores Plaintiff's and Class Members' PII.

37. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Citrix assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

38. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Citrix to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

39. Citrix could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members or by exercising due diligence in selecting their IT vendors and properly auditing those vendors' security practices.

40. Upon information and belief, Citrix made promises to Plaintiff and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

41. Citrix's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

42. Citrix's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PII, like Defendant, preceding the date of the breach.

43. Data thieves regularly target companies like Citrix's due to the highly sensitive information in their custody. Citrix knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

44. In 2021, a record 1,862 data breaches occurred, a 68% increase from 2020.[10]

45. Citrix was well aware that it was a target of cybercriminals, as it has repeatedly been the target of hackers from across the globe. For example, in October 2015 an infamous Russian hacker known as "w0rm" stated in a blog post that he was able to gain access to Citrix's content management system by exploiting weak credentials and was able to "gain access to admin functions including remote support."[11]

46. In June of 2016 GoToMyPC, a software service owned by Citrix was "targeted by a very sophisticated password attack" and in response required all customers to reset their passwords before logging into the service and encouraged customers to enable two-step verification as well as strong passwords to keep their accounts secure.[12]

47. In March 2019 Citrix was again the target of hackers, who according to security firm Resecurity, were able to obtain "access to at least 6 terabytes of sensitive data stored in the Citrix enterprise network, including e-mail correspondence, files in network shares and other services used for project management and procurement."[13] Ultimately, in April of 2019, Citrix notified affected individuals that the breach included "information related to certain individuals who are current and former employees, as well as certain beneficiaries and dependents. This

[10] *See* Identity Theft Resource Center's 2021 Data Breach Report, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last accessed January 10, 2024)
[11] https://www.theregister.com/2016/01/13/ruskie_hacker_pops_citrix/ (last accessed January 4, 2024)
[12] https://krebsonsecurity.com/2016/06/citing-attack-gotomypc-resets-all-passwords/ (last accessed January 4, 2024)
[13] https://www.forbes.com/sites/kateoflahertyuk/2019/03/10/citrix-data-breach-heres-what-to-do-next/?sh=686cc2191476 (last accessed January 4, 2024)

information may have included, for example, names, Social Security numbers, and financial information."[14]

48. As a custodian of PII, Citrix knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiff and Class members, and of the foreseeable consequences if their data security systems, or those of their vendors, were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

49. Despite the prevalence of public announcements of data breach and data security compromises, Citrix failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

50. At all relevant times, Citrix knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Citrix's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

51. Citrix was, or should have been, fully aware of the unique type and the significant volume of data on Citrix's server(s), amounting to potentially thousands of individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

52. The injuries to Plaintiff and Class Members were directly and proximately caused by Citrix's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

---

[14] Sample Notification letter provided to California Attorney General, https://oag.ca.gov/system/files/CX1%20US%20LTR%20%28no%20MA%20or%20CT%29_0.pdf (last accessed January 4, 2024)

53. The ramifications of Citrix's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

54. As a corporation in possession of its customers' and former customers' PII, Citrix knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Nevertheless, Citrix failed to take adequate cybersecurity measures to prevent the Data Breach.

55. As explained by the United States Army, "[f]or identity thieves, your name and Social Security number, credit card numbers or other financial account information are as good as gold…Skilled identity thieves may use a variety of methods to get a hold of your information…[t]hey may take your information from businesses or other institutions by…breaking into your records electronically."[15]

56. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[16]

57. The information compromised in the Data Breach carries more of a detriment to members than, for example, a retailer credit card breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names and Social Security numbers—meaning

[15] https://www.army.mil/article/74044/learn_to_detect_deter_and_defend_against_identity_theft (last accessed January 5, 2024)
[16] *See, e.g.* https://www.privacyaffairs.com/dark-web-price-index-2023/ (last accessed January 5, 2024); https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed January 5, 2024)

that Class Members must remain vigilant about future identity theft regardless of the passage of time.

58. Martin Walter, senior director at cybersecurity firm RedSeal, has explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[17]

59. Among other forms of fraud, identity thieves may open new lines of credit, obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

60. There may be a time lag between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

61. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[17] https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed January 5, 2024)

[18] GAO, Report to Congressional Requesters, at p.33 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf (emphases added) (last visited January 5, 2024).

62. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential customer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

63. As evidenced by the Data Breach, Citrix failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of their data security practices. Citrix's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

64. Citrix was at all times fully aware of their obligation to protect the PII of customers yet failed to comply with such obligations. Citrix was also aware of the significant repercussions that would result from their failure to do so.

65. In addition to its obligations under federal and state laws, Citrix owed a duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Citrix owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PII of Class Members.

66. Citrix breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems

and data and failed to audit, monitor, or ensure the integrity of its data security practices. Citrix's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

(i) Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

(ii) Failing to adequately protect customers' PII;

(iii) Failing to properly monitor its own data security systems for existing intrusions;

(iv) Failing to audit, monitor, or ensure the integrity of its vendors' data security practices;

(v) Failing to sufficiently train its customers and vendors regarding the proper handling of their customers' PII;

(vi) Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

(vii) Failing to adhere to industry standards for cybersecurity as discussed above; and

(viii) Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' PII.

67. Citrix negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

68. Had Citrix remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures

recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

69. As a result of Citrix's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including:

(i) invasion of privacy;

(ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk;

(iii) the loss of benefit of the bargain (price premium damages);

(iv) diminution of value of their PII;

(v) invasion of privacy; and

(vi) the continued risk to their PII, which remains in the possession of Citrix, and which is subject to further breaches, so long as Citrix fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

70. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

71. The unencrypted PII of Class Members will end up for sale on the dark web because that is the modus operandi of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

72. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

73. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

74. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

75. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" info.[19]

76. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. Even if certain information such as

[19] "Fullz info is a bundle of information that includes a "full" package for fraudsters [including] name, SSN, birth date, account numbers and other data that make them desirable since they can often do a lot of immediate damage." https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed January 5, 2024)

emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

77. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud.

78. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

79. These efforts are consistent with the U.S. Government Accountability Office which noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[20]

80. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[21]

[20] https://www.gao.gov/assets/gao-07-737.pdf p. 6 (last accessed January 5, 2024)
[21] https://www.identitytheft.gov/#/Steps (last accessed January 5, 2024)

81. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

82. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes—e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

83. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

84. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

85. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost

for a minimum of five years that Plaintiff and Class Members would not need to bear but for Citrix's failure to safeguard their PII.

86. Plaintiff Michelle Clark is a resident of New Jersey.

87. Plaintiff has been an Xfinity customer for more than two years.

88. In order to obtain Xfinity's services, Plaintiff was required to provide her PII to Xfinity, and indirectly to Citrix, including her name, date of birth, and Social Security number.

89. At the time of the Data Breach—between around October 16 and 19, 2023—Citrix retained Plaintiff's PII in their system.

90. Plaintiff is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted her PII to Citrix had she known of Citrix's lax data security policies.

91. On or about December 23, 2023 Plaintiff was notified by email from Xfinity that her personal information was involved in the data security incident described above. The notification indicated that the information in the breach included ""usernames and hashed passwords, for some customers, other information was also includes contact information, last four digits of social security numbers, date of birth and/or secret questions and answers.""[22] As a result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including checking her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

[22] *See* Data Breach Notice, Exhibit A.

92. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to:

(i) lost or diminished value of her PII;

(ii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time;

(iii) invasion of privacy;

(iv) loss of benefit of the bargain; and

(v) the continued and certainly increased risk to her PII, which:

a. remains unencrypted and available for unauthorized third parties to access and abuse; and

b. remains backed up in Citrix's possession and is subject to further unauthorized disclosures so long as Citrix fail to undertake appropriate and adequate measures to protect the PII.

93. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Citrix has still not fully informed her of key details about the Data Breach's occurrence.

94. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

95. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

96. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Citrix's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

97. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

98. Specifically, Plaintiff proposes the following class definition, subject to amendment as appropriate:

> All individuals in the United States whose PII was disclosed in the Data Breach (the "Class").

99. Excluded from the Class are Citrix and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

100. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

101. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

102. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes that the proposed Class includes millions of individuals who have been damaged by Citrix's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Citrix's records.

103. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

(i) Whether Citrix engaged in the conduct alleged herein;

(ii) Whether Citrix's conduct violated the FTCA;

(iii) When Citrix learned of the Data Breach;

(iv) Whether Citrix failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

(v) Whether Citrix's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

(vi) Whether Citrix's data security systems prior to and during the Data Breach were consistent with industry standards;

(vii) Whether Citrix's owed duties to Class Members to safeguard their PII;

(viii) Whether Citrix breached its duties to Class Members to safeguard their PII;

(ix) Whether hackers obtained Class Members' PII via the Data Breach;

(x) Whether Citrix had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

(xi) Whether Citrix breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

(xii) Whether Citrix knew or should have known its data security systems and monitoring processes were deficient;

(xiii) What damages Plaintiff and Class Members suffered as a result of Citrix's misconduct;

(xiv) Whether Citrix's conduct was negligent;

(xv) Whether Citrix breached contracts it had with its clients including Xfinity, of which Plaintiff and Class Members were third-party beneficiaries;

(xvi) Whether Citrix was unjustly enriched;

(xvii) Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

(xviii) Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

(xix) Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

104. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of Citrix. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

105. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

106. Predominance. Citrix has engaged in a common course of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Citrix's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

107. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Citrix. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

108. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Citrix has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

109. Finally, all members of the proposed Class are readily ascertainable. Citrix has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent a Notice Letter by Citrix.

CLAIMS FOR RELIEF
COUNT I
Negligence and Negligence Per Se
(On Behalf of Plaintiff and the Class)

110. Plaintiff restates and realleges paragraphs 1 through 109 above as if fully set forth herein.

111. Citrix's clients including Xfinity require their customers, including Plaintiff and Class Members, to submit non-public PII as a condition of obtaining services.

112. Citrix had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

113. By assuming the responsibility to collect and store this data, Citrix had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

114. Citrix had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

115. Citrix owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

116. Moreover, Citrix had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

117. Citrix had and continues to have duties to adequately disclose that the PII of Plaintiff and Class Members within Citrix's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

118. Citrix breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The

specific negligent acts and omissions committed by Citrix include, but are not limited to, the following:

(i) Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

(ii) Failing to adequately monitor the security of its networks and systems;

(iii) Failing to audit, monitor, or ensure the integrity of its vendors' data security practices;

(iv) Allowing unauthorized access to Class Members' PII;

(v) Failing to detect in a timely manner that Class Members' PII had been compromised;

(vi) Failing to remove former customers' PII it was no longer required to retain pursuant to regulations; and

(vii) Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

119. Citrix violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Citrix's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

120. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

121. Citrix's violation of Section 5 of the FTC Act constitutes negligence per se.

122. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

123. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Citrix's inadequate security practices.

124. It was foreseeable that Citrix's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches at large corporations.

125. Citrix had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

126. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Citrix knew or should have known of the inherent providing adequate security of that PII, and the necessity for encrypting PII stored on its systems.

127. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

128. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Citrix's possession.

129. Citrix was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

130. Citrix's duties extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the

actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

131. Citrix has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

132. But for Citrix's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

133. There is a close causal connection between Citrix's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII of Plaintiff and Class Members was lost and accessed as the proximate result of Citrix's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

134. As a direct and proximate result of Citrix's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

(i) invasion of privacy;

(ii) lost or diminished value of PII;

(iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach;

(iv) loss of benefit of the bargain;

(v) increase in spam calls, texts, and/or emails; and

(vi) the continued and certainly increased risk to their PII, which:

(a) remains unencrypted and available for unauthorized third parties to access and abuse; and

(b) remains backed up in Citrix's possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the PII.

135. As a direct and proximate result of Citrix's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

136. Additionally, as a direct and proximate result of Citrix's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Citrix's possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

137. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

138. Citrix's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

139. Plaintiff and Class Members are also entitled to injunctive relief requiring Citrix to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Class)

140. Plaintiff restates and realleges paragraphs 1 through 109 above as if fully set forth herein.

141. Citrix entered into contracts with its various clients to provide networking software to those clients.

142. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and Class Members, as it was their PII that Citrix agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and Class Members was the direct and primary objective of the contracting parties.

143. Citrix knew that if it were to breach these contracts with its clients, the clients' customers, including Plaintiff and Class Members, would be harmed by, among other things, fraudulent misuse of their PII.

144. Citrix breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII.

145. As a reasonably foreseeable result of the breach, Plaintiff and Class Members were harmed by Citrix's failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

146. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

147. Plaintiff restates and realleges paragraphs 1 through 109 above as if fully set forth herein.

148. This count is pleaded in the alternative to the Breach of Third-Party Beneficiary Contract claim above (Count II).

149. Plaintiff and Class Members conferred a monetary benefit on Citrix, in providing it, through Citrix's clients, with their valuable PII.

150. Citrix knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Citrix profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

151. Citrix failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

152. Citrix acquired the PII through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

153. If Plaintiff and Class Members had known Citrix would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would not have entrusted their PII to Citrix, through its clients.

154. Plaintiff and Class Members have no adequate remedy at law.

155. Under the circumstances, it would be unjust for Citrix to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

156. As a direct and proximate result of Citrix's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and

abuse; and (b) remains backed up in Citrix's possession and is subject to further unauthorized disclosures so long as Citrix fails to undertake appropriate and adequate measures to protect the PII.

157. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Citrix and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Citrix from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

158. Plaintiff and Class Members may not have an adequate remedy at law against Citrix, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, requests that the Court enter judgment against Citrix as follows:

A. An Order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is an appropriate representative of the Class requested herein;

B. Equitable relief compelling Citrix to utilize appropriate methods and policies with respect to consumer data collection, storage and safety, and requiring disclosure with specificity to Class Members the information disclosed.

C. Injunctive relief including, but not limited to an Order requiring Citrix to:

(i) Delete the personal identifying information of Plaintiff and all Class Members;

(ii) Strengthen its data security systems that maintain personal identifying information to comply with all applicable regulations, state and federal laws as well as best practices under industry standards;

(iii) Engage third-party auditors and internal personnel to conduct security testing and audits on Citrix's systems on a regular basis;

(iv) Promptly correct any problems or issues detected by such audits and testing;

(v) Routinely and continually conduct training to inform security personnel how to prevent, identify and contain a breach, and how to appropriately respond.

D. An award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. An award of punitive damages, as allowable by law;

F. An award of attorneys' fees and costs, and any other expenses, including expert witness fees and the costs associated with Class notice and administration of Class-wide relief;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: January 19, 2024

Respectfully submitted,

/s/ *David M. Buckner*
David M. Buckner
Florida Bar No. 060550
david@bucknermiles.com
BUCKNER + MILES
2020 Salzedo Street, Suite 302
Coral Gables, Florida 33134
Telephone: 305.964.8003
Facsimile: 786.523.0485

James A. Barry, Esq.*
POGUST GOODHEAD LLC
505 S. Lenola Rd., Suite 126
Moorestown, NJ 08057
jbarry@pogustgoodhead.com
Telephone: (610) 941-4204

Meghan J. Talbot, Esq.*
161 Washington St., Ste. 250
Conshohocken, PA 19428
mtalbot@pogustgoodhead.com
Telephone: (610) 941-4204

Michael A. Galpern, Esq.*
Javerbaum Wurgaft Hicks Kahn
Wikstrom & Sinins, P.C.
1000 Haddonfield-Berlin Road, Suite 203
Voorhees, NJ 08043
mgalpern@lawjw.com
Telephone: (856) 596-4100

**pro hac vice to be filed*

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing was served by CM/ECF on January 19, 2024, on all counsel or parties of record on the Service List below.

/s/David M. Buckner
David M. Buckner, Esq.
Florida Bar No. 060550
david@bucknermiles.com